Despliegue y Análisis de T-Pot Honeypot

Presenter Name
Alejandro García
Maximiliano Altamirano
Alvaro Munilla

Entendiendo T-Pot

T-Pot es:

una plataforma de honeypots de código abierto basada en contenedores Docker, diseñada para detectar, registrar y analizar ataques en tiempo real.

Ayuda a la investigación y la prevención.

Ayuda a mejorar las medidas de seguridad basándose en los datos recopilados.

Recopila datos sobre ataques

Proporciona información sobre patrones y técnicas de ataque.

T-Pot admite múltiples servicios.

Integra varias herramientas para realizar análisis de seguridad exhaustivos.

Fases del Proyecto T-Pot

Un desglose detallado de cada etapa en el despliegue y análisis de T-Pot.

Instalación local de T-Pot y exploración inicial.

Fundamental para probar TPoT

Selección de honeypots a implementar para un análisis efectivo.

Clave para estudiar amenazas específicas.

Configuración integral, personalización/optimización del sistema y despliegue en la nube

Ajustes necesarios para un rendimiento óptimo.

Recolección y análisis de datos para informes precisos.

Estudio de los logs obtenidos

Proceso de Configuración de T-Pot Honeypot

Instalación y configuración de T-Pot en un entorno local.

1

Clonación del repositorio T-Pot

2

Ejecución del instalador

3

Selección de instalación estándar (Hive)

4

Configuración de credenciales

Personalización y Despliegue de T-Pot

Personalización del sistema T-Pot y validación de su funcionamiento.

Ejecutar el script customizer.py para personalizar T-Pot.

Lanzamos el script **customizer.py** desde el directorio **/tpotce/compose** para aplicar las configuraciones personalizadas necesarias en el sistema.

Copiar el archivo docker-compose personalizado.

Trasladamos el fichero **docker-compose-custom.yml** al directorio **/tpotce/**, asegurando que la configuración personalizada esté disponible.

Validar la configuración de T-Pot.

Ejecutamos **docker-compose** para iniciar el sistema con la configuración personalizada, verificando su correcto funcionamiento.

Verificar el inicio del sistema.

Al ejecutar **docker-compose -f docker-compose-custom.yml up**, observamos los logs para confirmar que todos los servicios de T-Pot se inician sin errores.

Despliegue y Configuración de T-Pot en AWS

Implementación de T-Pot Honeypot utilizando recursos de AWS para un análisis efectivo.

1. **Seleccionamos servidores de AWS**

   Utilizamos servidores de **AWS** por su capacidad de ofrecer configuraciones amplias de conectividad y recursos adecuados para nuestras necesidades de despliegue.

2. **Recursos recomendados para la instancia**

   Se recomienda una configuración inicial de **16GB RAM** y **150GB** de almacenamiento para asegurar un rendimiento óptimo del sistema y de los **Honeypots**.

3. **Generación de claves SSH únicas**

   Creamos un par de claves únicas para el acceso **SSH** externo, asegurando que la conexión sea segura y controlada desde el exterior.

4. **Puertos de monitoreo configurados**

   Configuramos los puertos **64295** para **SSH** y **64297** para acceder a la interfaz web de **T-Pot**, lo que permite un monitoreo efectivo del sistema.

5. **Exposición de múltiples Honeypots**

   Exponemos **T-Pot** con múltiples **Honeypots** y validamos la conexión externa, facilitando la captación de datos y el análisis de intrusiones.

6. **Validación de conexión externa**

   Realizamos pruebas para validar la conexión externa a **T-Pot**, asegurando que el sistema esté accesible y funcional desde el exterior.

Honeypots

Honeypots desplegados y analisis de resultados

En esta sección, describimos la configuración y personalización de los honeypots a utilizar

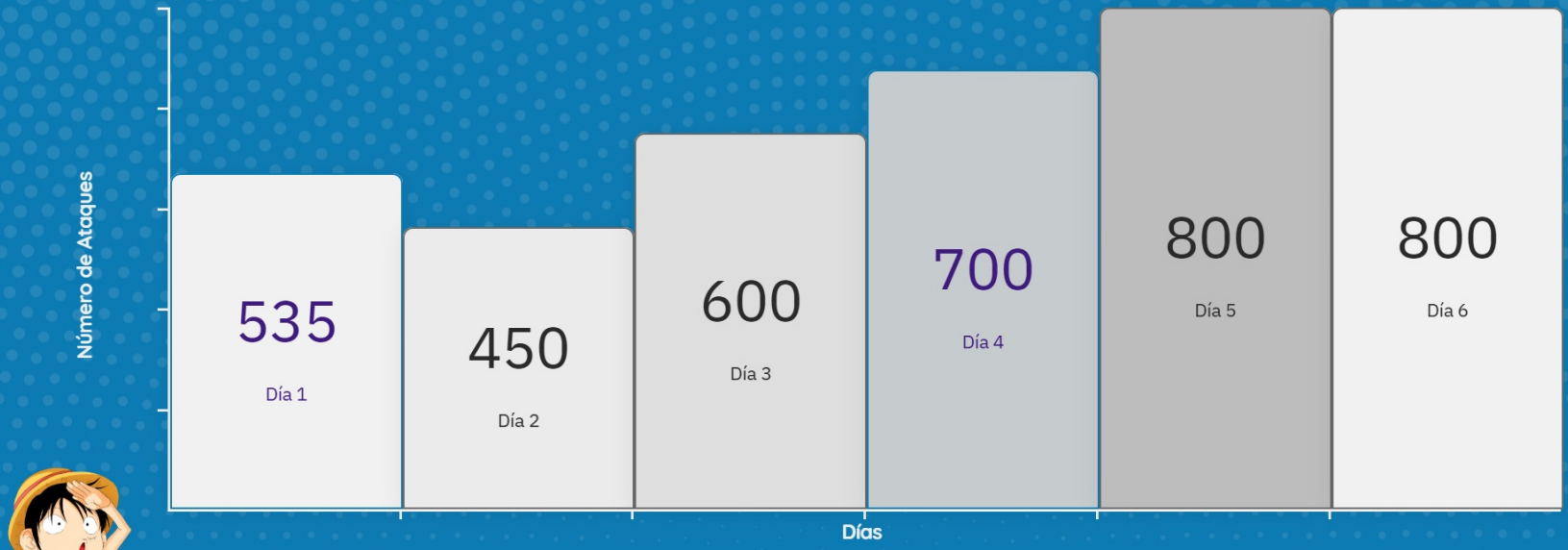
Honeypots desplegadas

Honeypots	¿Por qué los hemos elegido?
Cowrie	Simula un sistema SSH y Telnet vulnerable, registrando intentos de acceso, comandos ejecutados y técnicas de intrusión. Es útil para estudiar las tácticas, técnicas y procedimientos (TTPs).
Dionaea	Emula múltiples servicios (SMB, FTP, HTTP, etc.) para atraer malware y registrar payloads maliciosos, facilitando el análisis forense.
Conpot	Simula sistemas SCADA/ICS (Industrial Control Systems) para detectar ataques dirigidos a infraestructuras críticas, permitiendo estudiar ataques específicos contra sistemas industriales.
Elasticpot	Integra datos del honeypot en Elasticsearch para análisis avanzado y visualización en Kibana.
Honeytrap	Ofrece una plataforma flexible para crear honeypots personalizados en diferentes protocolos o servicios.
Mailoney	Detecta campañas de spam o phishing mediante la captura de correos electrónicos maliciosos o sospechosos.
WordPot	Captura intentos de explotación relacionados con vulnerabilidades en WordPress u otros CMS similares.
DDoSPot	Detecta y analizar ataques DDoS dirigidos a la infraestructura del honeypot o red protegida.
Suricata	Analiza tráfico capturado o en tránsito usando reglas específicas para identificar amenazas.
Kibana	Visualiza datos almacenados en Elasticsearch para detectar patrones o incidentes rápidamente.
Elasticsearch	Almacena grandes volúmenes de datos generados por los honeypots para facilitar búsquedas y análisis.

Análisis de Ataques a Honeypots T-Pot

Estadísticas sobre la actividad de ataques en Honeypots como Honeytrap y Glutton

Distribución Diaria De Ataques: 2h*Dia



s recogidos de T-Pot

Reflexiones sobre el proyecto

¿Qué os ha aportado desarrollar este proyecto? ¿Qué habéis aprendido?

¿Qué no volveríais a hacer?

¿Qué seguiríais haciendo en el futuro?

¡Muchas gracias a todos!

¿Preguntas?